

ACKSYS OpenVPN 설정 매뉴얼

[적용모델]

	RuggedAir 시리즈
	RailBox 시리즈
	AirRoad
	AirBox 시리즈
	AirLink
	EmbedAir 시리즈

1. 구성도 및 개요

2. OpenVPN 서버 설정

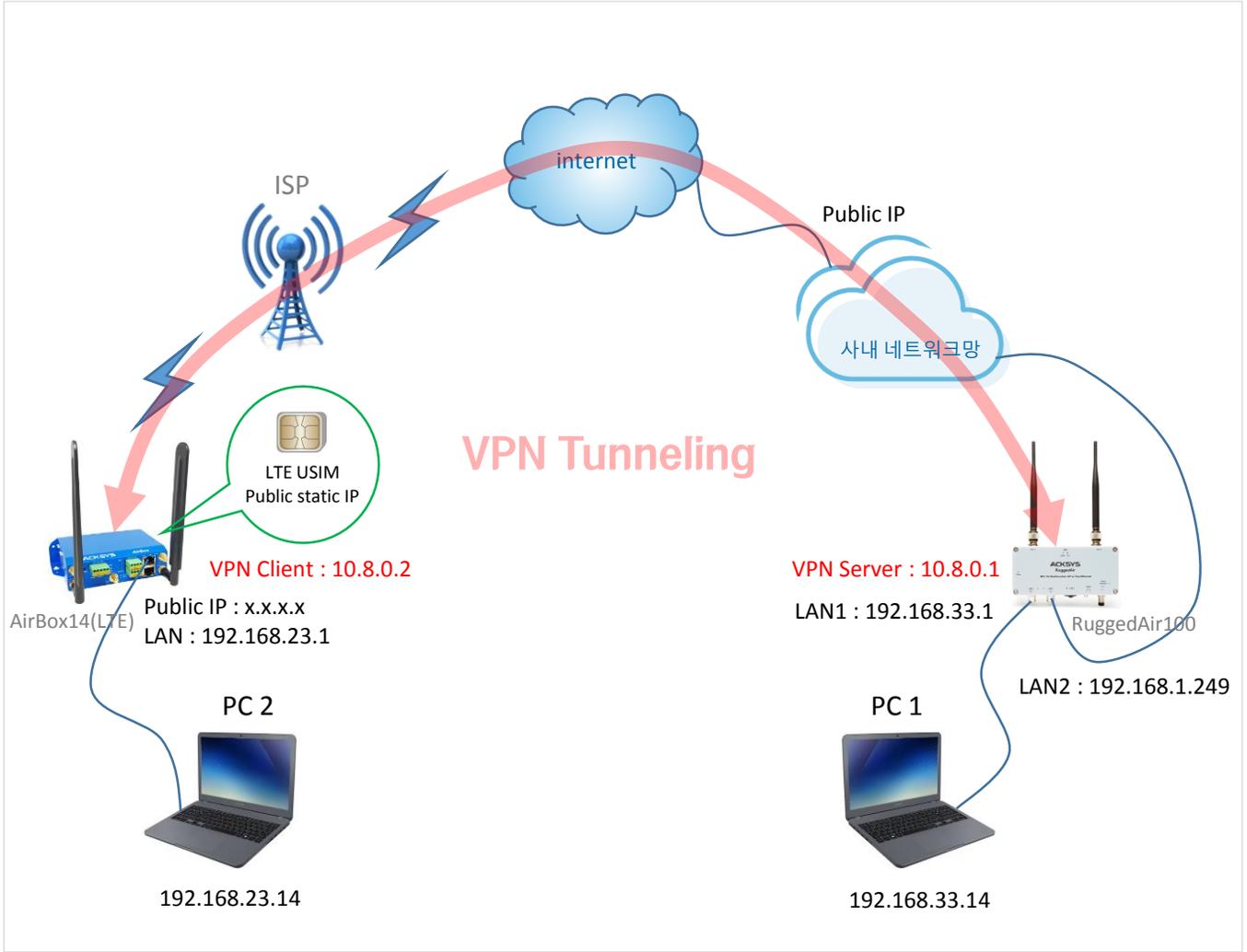
- NETWORK
- VPN
- NETWORK ZONES

3. OpenVPN 클라이언트 설정

- NETWORK
- VPN
- NETWORK ZONES

4. OpenVPN 터널링 확인 (서버)

5. OpenVPN 터널링 확인 (클라이언트)



ACKSYS 제품을 통해 cellular VPN client가 사무실 백본에 있는 VPN 서버에 연결되는 예시입니다.

사내 네트워크망에서는 VPN 클라이언트의 트래픽이 VPN 서버에 전달될 수 있도록 라우터에 포트포워딩 규칙(여기서는 1194 포트)을 설정해주세요. 인증서와 키없이 터널을 구축하여 간단하게 테스트를 하고, 그 이후 인증과 암호화를 추가하여 테스트 합니다.

가입한 LTE 상품에 따라 고정공인 IP 또는 사설유동 IP를 부여받을 수 있으며, 이에 따라 AirBox14(LTE) 제품은 서버 또는 클라이언트로 동작되어 거리에 제한 없이 LTE망을 통해 적절한 네트워크망을 구축하실 수 있습니다.

윈도우 PC에서는 기본적으로 방화벽에 의해 ping 응답이 비활성화 되어 있으므로 들어오는 ping 트래픽을 허용하는 규칙을 추가하세요. PC1과 PC2는 아래처럼 설정하실 수 있으며, 이 매뉴얼에서의 모든 IP는 네트워크 환경에 따라 적절하게 변경하실 수 있습니다.

구분	PC1		PC2	
IP	192.168.33.14		192.168.23.14	
Subnet Mask	255.255.255.0		255.255.255.0	
Gateway	192.168.33.1		192.168.23.1	
DNS	기본	168.126.63.1	기본	211.36.129.4
	보조	168.126.63.2	보조	117.111.29.4

SETUP > NETWORK

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES
 VIRTUAL INTERFACES
NETWORK
 LAN
 WAN
 VPN
 BRIDGING
 ROUTING / FIREWALL

NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LAN	<input checked="" type="checkbox"/>	192.168.33.1	255.255.255.0		Enabled	
WAN	<input checked="" type="checkbox"/>	192.168.1.249	255.255.255.0	192.168.1.1 (0)	Default	

Add network

(설정이 완료된 화면)

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interface network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Enable interface

Network description Friendly name for your net

Protocol

IPv4-Address

IPv4-Netmask

Default IPv4 gateway

Default gateway metric Gateway priority when sev (Used only when a default gate

DNS server(s) You can specify multiple D

Network의 LAN IP를 static으로 설정합니다. gateway는 생략되어도 됩니다.

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interface network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Bridge interfaces creates a bridge over

Enable STP/RSTP Enables the Spanni **WARNING: Some cautions**

Enable LLDP forwarding Enables the LLDP fi

bridge VLAN Enable VLAN mana
 >bridging)

Interface WiFi adap
 Ethernet t
 Ethernet t

MTU

Bridge interfaces 및 Interface 설정(LAN1)을 체크합니다.

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Network persistence Avoid the netwo

State at startup Default is 'up' ex Use 'down' if this net

기본 설정을 유지합니다.

SETUP > NETWORK

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES
 VIRTUAL INTERFACES
NETWORK
 LAN
 WAN
 VPN
 BRIDGING
 ROUTING / FIREWALL

NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LAN	<input checked="" type="checkbox"/>	192.168.33.1	255.255.255.0		Enabled	
WAN	<input checked="" type="checkbox"/>	192.168.1.249	255.255.255.0	192.168.1.1 (0)	Default	

+ Add network

(설정이 완료된 화면)

NETWORK - WAN

On this page you can configure the network interfaces. You can bridge several inter network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Enable interface

Network description Friendly name for your

Protocol

IPv4-Address

IPv4-Netmask

Default IPv4 gateway

Default gateway metric Gateway priority when (Used only when a default

DNS server(s)

Add network를 클릭하여 Network의 WAN IP를 static으로 설정합니다. 해당 네트워크의 gateway를 기입합니다.

NETWORK - WAN

On this page you can configure the network interfaces. You can bridge several inter network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Bridge interfaces creates a bridge i

Interface WiFi ac Ethernet Ethernet

MTU

Bridge interfaces 체크 해제 및 Interface 설정(LAN2)을 체크합니다.

NETWORK - WAN

On this page you can configure the network interfaces. You can bridge sev network interfaces.

COMMON CONFIGURATION

General Setup
Interfaces Settings
Advanced Settings

Network persistence Avoid the n

State at startup Default is '\ Use 'down' if thi

두 항목을 Default로 설정합니다.

SETUP > VPN

SETUP TOOLS STATUS

PHYSICAL INTERFACES
VIRTUAL INTERFACES
NETWORK
VPN
VPN1
BRIDGING

OPENVPN INSTANCES OVERVIEW

NAME	ENABLED	MODE	PROTOCOL	SECURITY	ACTIONS
vpn1	<input checked="" type="checkbox"/>	Server	tcp/1194	none	

Add instance

(설정이 완료된 화면)

SETUP TOOLS STATUS

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a

CONFIGURATION

Tunnel settings | Auth/Crypto | Server settings

Enable virtual network

State at startup Up

OpenVPN instance description vpn1

Role Server (called)

Protocol TCP

Listener port 1194

Data channel compression Use fast LZO compression

Tunnel type L3 (IP) tunnel

VPN subnet local IP address 10.8.0.1

VPN subnet mask 255.255.255.0

Keepalive period 10

Keepalive timeout 30

서버 설정 및 TCP, 통신포트 1194를 설정합니다.

LOCAL ROUTES

This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.

- In the client, it lists the server subnets reachable using the server as gateway,
- In the server, it lists the client subnets reachable using the client as gateway.

If the gateway is not indicated, it defaults to the VPN remote address.

TARGET NET	NETMASK	GATEWAY	
192.168.23.0	255.255.255.0	10.8.0.2	Default: 0

클라이언트 네트워크 대역 및 게이트웨이를 설정합니다.

SETUP > VPN

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

VPN

VPN1

BRIDGING

ROUTING / PROXIMA

OPENVPN INSTANCES OVERVIEW

NAME	ENABLED	MODE	PROTOCOL	SECURITY	ACTIONS
vpn1	<input checked="" type="checkbox"/>	Server	tcp/1194	none	

Add instance

(설정이 완료된 화면)

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a p...

CONFIGURATION

Tunnel settings

Auth/Crypto

Server settings

Key type No key (entails P2P, cleartext, no auth) ▼

Data channel authentication digest SHA1 (OpenVPN default) ▼

Data channel authentication algorithm. Adds overhead to frames size

간단한 테스트를 위해 인증서와 키 없이 설정을 진행합니다.

LOCAL ROUTES

This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.

- In the client, it lists the server subnets reachable using the server as gateway,
- In the server, it lists the client subnets reachable using the client as gateway.

If the gateway is not indicated, it defaults to the VPN remote address.

TARGET NET	NETMASK	GATEWAY	
192.168.23.0	255.255.255.0	10.8.0.2	Default: 0

SETUP > ROUTING/FIREWALL > NETWORK ZONES

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
LAN_zone	"LAN"	VPN_zone WAN_zone	<input type="checkbox"/>	All enabled	
VPN_zone	vpn1	LAN_zone WAN_zone	<input type="checkbox"/>	All enabled	
WAN_zone	"WAN"	-	<input type="checkbox"/>	All enabled	

Add zone

(설정이 완료된 화면)

NETWORK ZONES - ZONE SETTINGS

ZONE "LAN_ZONE"

This section defines common properties of "LAN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: LAN_zone

Enable NAT: Only on public zones. Warn

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the local

Covered networks:

- LAN:
- WAN:
- vpn1:

위의 Add zone을 클릭하여 LAN_zone을 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (LAN_zone) and other zones. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a

Allow forwarding to destination zones:

- VPN_zone vpn1:
- WAN_zone WAN:

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

LAN_zone을 먼저 생성하고 각 영역을 생성한 후에 체크합니다.

NETWORK ZONES - ZONE SETTINGS

ZONE "VPN_ZONE"

This section defines common properties of "VPN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: VPN_zone

Enable NAT: Only on public zones. Warn

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the local

Covered networks:

- LAN:
- WAN:
- vpn1:

위의 Add zone을 클릭하여 VPN_zone을 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (VPN_zone) and other zones. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a

Allow forwarding to destination zones:

- LAN_zone LAN:
- WAN_zone WAN:

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

VPN_zone을 생성하고 각 영역을 생성한 후에 체크합니다.

SETUP > ROUTING/FIREWALL > NETWORK ZONES

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
LAN_zone	"LAN"	VPN_zone WAN_zone	<input type="checkbox"/>	All enabled	
VPN_zone	vpn1	LAN_zone WAN_zone	<input type="checkbox"/>	All enabled	
WAN_zone	"WAN"	-	<input type="checkbox"/>	All enabled	

Add zone

(설정이 완료된 화면)

ZONE "WAN_ZONE"

This section defines common properties of "WAN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: WAN_zone

Enable NAT: Only on public zones. Wa

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the loc

Covered networks:

- LAN:
- WAN:
- vpn1:

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (WAN_zone) and other zones: "WAN_zone". The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply

Allow forwarding to destination zones:

- LAN_zone LAN:
- VPN_zone vpn1:

위의 Add zone을 클릭하여 WAN_zone을 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

기존에 생성한 영역의 체크를 해제합니다.

SETUP > NETWORK

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LOCAL	<input checked="" type="checkbox"/>	192.168.23.1	255.255.255.0	(0)	Enabled	
Cellular	<input checked="" type="checkbox"/>	DHCP		DHCP (0)	Default	WAN config.

공인 IP는 보안상 블라인드 처리되었습니다.

(설정이 완료된 화면)

위의 Add network를 클릭하여 Network의 Local IP를 static으로 설정합니다.

gateway는 LTE에서 주어진 IP를 입력합니다.
DNS는 사용하고 있는 통신사 DNS를 기입합니다.

Bridge interfaces 및 Interface 설정(LAN1)을 체크합니다.
Interface WiFi 부분은 체크 해제하셔도 무방합니다.
(추후 사용 시 체크 필요)

기본 설정을 유지합니다.

SETUP > NETWORK

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LOCAL	<input checked="" type="checkbox"/>	192.168.23.1	255.255.255.0	(0)	Enabled	[edit]
Cellular	<input checked="" type="checkbox"/>	DHCP		DHCP (0)	Default	WAN config.

[Add network](#)

공인 IP는 보안상 블라인드 처리되었습니다.

(설정이 완료된 화면)

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

Network description: Cellular

Default SIM card: SIM 1 SIM 2

Protocol: DHCP

Replace default route:

Default gateway metric: 0

위의 Add network를 클릭하여 Network의 Cellular를 기본값으로 설정합니다.

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

SIM card 1 PIN code: [masked]

SIM card 1 access point (APN): m2m-static-server.lguplus.co.kr

Authentication protocol: SIM only

SIM 카드에 주어진 핀번호를 입력 후 APN을 기입합니다.

<LG U+ APN>
m2m-static-server.lguplus.co.kr

<KTmMobile APN>
lte.ktfwing.com

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

Always disabled at startup:

State at startup: Default

Log AT transactions at "debug" level:

그림과 같이 기본값으로 진행합니다.

SETUP > VPN

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

VPN

VPN1

BRIDGING

ROUTING / SERIAL

OPENVPN INSTANCES OVERVIEW

NAME	ENABLED	MODE	PROTOCOL	SECURITY	ACTIONS
vpn1	<input checked="" type="checkbox"/>	Client	tcp/1194	none	

Add instance

(설정이 완료된 화면)

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a predefined OpenVPN server address.

CONFIGURATION

Tunnel settings
Auth/Crypto
Client settings

Enable virtual network

State at startup Up

Default is 'up' except for networks with protocol 'none'.
Use 'down' if this network should be brought up only by event rules.

OpenVPN instance description

Friendly name for this VPN instance

Role Client (calling)

Protocol TCP

Favor UDP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms

Listener port 1194

UDP or TCP port that the server will listen to, and that the client will call

Data channel compression Use fast LZO compression

Tunnel type L3 (IP) tunnel

Only L3 tunnels are supported

VPN subnet local IP address

IP address of the local VPN endpoint, not used in TLS client mode since it is pulled from server

VPN subnet mask

Subnet mask of the VPN subnet, not used in TLS client mode

Keepalive period

Keepalive period (seconds). Every such time, a packet is sent to each peer to elicit a response.

Keepalive timeout

Keepalive timeout (seconds). Connection terminates if no traffic is received from the peer for such time.

클라이언트 설정 및 TCP, 통신포트 1194를 설정합니다.

LOCAL ROUTES

This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.

- In the client, it lists the server subnets reachable using the server as gateway.
- In the server, it lists the client subnets reachable using the client as gateway.

If the gateway is not indicated, it defaults to the VPN remote address.

TARGET NET	NETMASK	GATEWAY	METRIC	SORT	
<input type="text" value="192.168.33.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="10.8.0.1"/>	<input type="text" value="Default: 0"/>	+ +	

Add

서버 네트워크 대역 및 게이트웨이를 설정합니다.

SETUP > VPN

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES
VIRTUAL INTERFACES
NETWORK
VPN
VPN1
BRIDGING
ROUTING / FIREWALL

OPENVPN INSTANCES OVERVIEW

NAME	ENABLED	MODE	PROTOCOL	SECURITY	ACTIONS
vpn1	<input checked="" type="checkbox"/>	Client	tcp/1194	none	✎ ✖

+ Add instance

공인 IP는 보안상 블라인드 처리되었습니다.

(설정이 완료된 화면)

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a pr

CONFIGURATION

Tunnel settings
Auth/Crypto
Client settings

Key type No key (entails P2P, cleartext, no auth) ▼

Data channel authentication digest SHA1 (OpenVPN default) ▼
 ⓘ Data channel authentication algorithm. Adds overhead to frames size

간단한 테스트를 위해 인증서와 키 없이 설정을 진행합니다.

LOCAL ROUTES

This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.

- In the client, it lists the server subnets reachable using the server as gateway.
- In the server, it lists the client subnets reachable using the client as gateway.

If the gateway is not indicated, it defaults to the VPN remote address.

TARGET NET	NETMASK	GATEWAY	
192.168.33.0	255.255.255.0	10.8.0.1	Default: 0

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a

CONFIGURATION

Tunnel settings
Auth/Crypto
Client settings

Remote OpenVPN server address [Redacted]
 ⓘ Remote OpenVPN server address

OpenVPN 서버가 사용하는 공인 IP를 입력합니다.

SETUP > ROUTING/FIREWALL > NETWORK ZONES

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
LOCAL	"LOCAL"	LTE VPN_zone	<input type="checkbox"/>	All enabled	
LTE	"Cellular"	-	<input checked="" type="checkbox"/>	All enabled	
VPN_zone	vpn1	LOCAL LTE	<input type="checkbox"/>	All enabled	

Add zone

(설정이 완료된 화면)

NETWORK ZONES - ZONE SETTINGS

ZONE "LOCAL"

This section defines common properties of "LOCAL".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: LOCAL

Enable NAT: Only on public zones. Warning

MSS clamping:

Default acceptance policy for local services: All enabled

Covered networks:

- LOCAL:
- vpn1:
- Cellular:

위의 Add zone을 클릭하여 LOCAL을 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (LOCAL) and other zones. Destination forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan.

Allow forwarding to destination zones:

- LTE Cellular:
- VPN_zone vpn1:

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

LOCAL을 먼저 생성하고 각 영역을 생성한 후에 체크합니다.

NETWORK ZONES - ZONE SETTINGS

ZONE "VPN_ZONE"

This section defines common properties of "VPN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: VPN_zone

Enable NAT: Only on public zones. Warning

MSS clamping:

Default acceptance policy for local services: All enabled

Covered networks:

- LOCAL:
- vpn1:
- Cellular:

위의 Add zone을 클릭하여 VPN_zone을 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (VPN_zone) and other zones. Destination forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan.

Allow forwarding to destination zones:

- LOCAL LOCAL:
- LTE Cellular:

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

VPN_zone을 생성하고 각 영역을 생성한 후에 체크합니다.

SETUP > ROUTING/FIREWALL > NETWORK ZONES

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
LOCAL	"LOCAL"	LTE VPN_zone	<input type="checkbox"/>	All enabled	
LTE	"Cellular"	-	<input checked="" type="checkbox"/>	All enabled	
VPN_zone	vpn1	LOCAL LTE	<input type="checkbox"/>	All enabled	

Add zone

(설정이 완료된 화면)

NETWORK ZONES - ZONE SETTINGS

ZONE "LTE"

This section defines common properties of "LTE".
Covered networks specifies which available networks are members of this zone.

General Settings | **Advanced Settings**

Name: LTE

Enable NAT: Only on public zones. **Warning**

MSS clamping:

Default acceptance policy for local services: All enabled

Covered networks:

- LOCAL
- vpn1
- Cellular

위의 Add zone을 클릭하여 LTE를 설정합니다.

커버하는 네트워크는 해당 영역을 선택합니다.

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (LTE) and other zones. *Destination forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward*

Allow forwarding to destination zones:

- LOCAL LOCAL:
- VPN_zone vpn1:

이 부분은 각 네트워크 영역을 생성한 후에 나타납니다.

기존에 생성한 영역의 체크를 해제합니다.

OpenVPN 서버와 클라이언트가 서로 통신을 하기 위한 설정이 모두 끝났습니다.
이제 제품의 상태와 로그 자료를 통해 연결이 잘 되었는지 확인하실 수 있습니다.

STATUS > NETWORK

SETUP
TOOLS
STATUS

DEVICE INFO

NETWORK

BRIDGES

MULTICAST ROUTES

ROUTES

WIRELESS

SERVICES

LOGS

INTERFACES

LAN

IP CONFIGURATION

IPv4: 192.168.33.1 Netmask: 24 MTU: 1500

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN 1	00:09:90:01:06:63	1463044	1648575	Negotiated 100 baseTX FD, link ok	1500

WAN

IP CONFIGURATION

IPv4: 192.168.1.249 Netmask: 24 MTU: 1500

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN 2	00:09:90:01:06:64	2168743	2607354	Negotiated 100 baseTX FD, link ok	1500

VPN1 (VPN1)

CONNECTED PEERS

COMMON NAME	REAL ADDRESS	BYTES RECEIVED	BYTES SENT
Not available	(null)	699333	722179

ROUTES

The following rules are currently active on this system.

ACTIVE IPv4-ROUTES

NETWORK	TARGET	IPv4-NETMASK	IPv4-GATEWAY	METRIC
WAN	default	0.0.0.0	192.168.1.1	0
vpn1	10.8.0.0	255.255.255.0	local	0
WAN	192.168.1.0	255.255.255.0	local	0
vpn1	192.168.23.0	255.255.255.0	10.8.0.2	0
LAN	192.168.33.0	255.255.255.0	local	0

SYSTEM LOG

Save logs to file

```

Mon Apr 1 20:20:20 2019 kern.err kernel: [ 0.604000] Unknow marvell switch ident fff0
Mon Apr 1 20:20:20 2019 kern.err kernel: [ 0.620000] Unknow marvell switch ident fff0
Mon Apr 1 20:20:20 2019 kern.err kernel: [ 1.200000] Unknow marvell switch ident fff0
Mon Apr 1 20:20:20 2019 kern.err kernel: [ 1.772000] Unknow marvell switch ident fff0
Mon Apr 1 20:20:29 2019 daemon.err acksys_event_handlerd: acksys_event_handlerd: Cannot open /sys/class/gpio/digital_out1/value, alarm '2'
Mon Apr 1 20:20:29 2019 daemon.err acksys_event_handlerd: acksys_event_handlerd: Alarm '2' not available, not set/cleared
Mon Apr 1 20:20:31 2019 daemon.err block: /dev/ubi0_2 is already mounted
Mon Apr 1 20:20:56 2019 daemon.err acksys_event_handlerd: acksys_event_handlerd: gnss action start_events failed (Not found)
    
```

경기도 용인시 기흥구 구성로 357, 용인테크노밸리 C동 707호 (주)와이트리 T : 031-215-2263 / F : 031-624-2260 www.witree.co.kr info@witree.co.kr

SETUP TOOLS **STATUS**

INTERFACES

LOCAL

IP CONFIGURATION						
IPv4: 192.168.23.1 Netmask: 24 MTU: 1500						
DNS server: 211.36.129.4 117.111.29.4						
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN1	00:09:90:01:1d:3b	13964211	3150997	Negotiated 1000 baseTX FD, link ok	1500

VPN1 (VPN1)

CONNECTED PEERS			
COMMON NAME	REAL ADDRESS	BYTES RECEIVED	BYTES SENT
Not available		1247641	1751625

CELLULAR

IP CONFIGURATION						
IPv4: Netmask: 28 MTU: 1500						
DHCP info: Lease time: 7200s						
DNS server: 211.36.129.4 117.111.29.4						
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	Cellular	00:00:00:00:00:00	4966436	14962637	Operator (home): LG U+ LGU+ SIM: Password accepted	1500

SETUP TOOLS **STATUS**

ROUTES

The following rules are currently active on this system.

ACTIVE IPV4-ROUTES

NETWORK	TARGET	IPV4-NETMASK	IPV4-GATEWAY	METRIC
Cellular	default	0.0.0.0	223.171.58.9	0
vpn1	10.8.0.0	255.255.255.0	local	0
LOCAL	192.168.23.0	255.255.255.0	local	0
vpn1	192.168.33.0	255.255.255.0	10.8.0.1	0
Cellular	223.171.58.0	255.255.255.240	local	0

SYSTEM LOG

Save logs to file

```
Tue Mar 24 17:27:16 2020 daemon.info dnsmasq[1932]: using nameserver 211.36.129.4#53
Tue Mar 24 17:27:16 2020 daemon.info dnsmasq[1932]: using nameserver 117.111.29.4#53
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'loopback' is enabled
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'loopback' is setting up now
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'loopback' is now up
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'vpn1' is setting up now
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'wwan0' is setting up now
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Network device 'cpu0' link is up (called from cb_rtnl_event:carrier)
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Network device 'lo' link is up (called from cb_rtnl_event:carrier)
Tue Mar 24 17:27:16 2020 daemon.notice netifd: Interface 'loopback' has link connectivity
Tue Mar 24 17:27:17 2020 kern.info kernel: [ 39.345571] dsa dsa.0 eth0: Link is Down
Tue Mar 24 17:27:17 2020 daemon.err uhttpd[2624]: socket(): Address family not supported by protocol
Tue Mar 24 17:27:17 2020 daemon.notice netifd: wwan0 (2580): wwan0[2580] Using proto:wwan device:/dev/cdc-wdm0 iface:wwan0 desc:Quectel EC
Tue Mar 24 17:27:17 2020 daemon.info wwan0: proto qmi acksys ql setup wwan0
Tue Mar 24 17:27:17 2020 daemon.notice openvpn(vpn1)[2623]: OpenVPN 2.3.10 mips-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv
Tue Mar 24 17:27:17 2020 daemon.notice openvpn(vpn1)[2623]: library versions: OpenSSL 1.0.2p 14 Aug 2018, LZO 2.10
Tue Mar 24 17:27:17 2020 daemon.warn openvpn(vpn1)[2623]: NOTE: the current --script-security setting may allow this configuration to call
Tue Mar 24 17:27:17 2020 daemon.warn openvpn(vpn1)[2623]: ***** WARNING *****: all encryption and authentication features disabled --
Tue Mar 24 17:27:17 2020 daemon.notice openvpn(vpn1)[2623]: TUN/TAP device tun0 opened
Tue Mar 24 17:27:17 2020 daemon.notice openvpn(vpn1)[2623]: /etc/openvpn/scripts/if-up vpn1 tun0 1500 1503 10.8.0.2 255.255.255.0 init
Tue Mar 24 17:27:18 2020 daemon.notice netifd: wwan0 (2580): Setting up wwan0
Tue Mar 24 17:27:19 2020 daemon.notice netifd: Network device 'tun0' link is up (called from cb_if_check_valid)
Tue Mar 24 17:27:19 2020 daemon.notice netifd: Interface 'vpn1' is now up
Tue Mar 24 17:27:19 2020 user.info quectel-CM: Cellular: localtime=1585038439,operator=,loc=421E,cellid=0E38421,mode=7
Tue Mar 24 17:27:19 2020 user.info quectel-CM: Cellular: localtime=1585038439,operator=LG U+ LGU+,loc=421E,cellid=0E38421,mode=7
Tue Mar 24 17:27:19 2020 user.notice firewall: Reloading firewall due to ifup of lan (br-lan)
Tue Mar 24 17:27:19 2020 daemon.notice openvpn(vpn1)[2623]: Attempting to establish TCP connection with [AF_INET] :1194 [nonb
Tue Mar 24 17:27:19 2020 daemon.err openvpn(vpn1)[2623]: TCP: connect to [AF_INET] :1194 failed, will try again in 5 seconds:
Tue Mar 24 17:27:20 2020 user.info quectel-CM: Cellular: localtime=1585038440,operator=LG U+ LGU+,loc=421E,cellid=0E38F19,mode=7
Tue Mar 24 17:27:20 2020 user.info quectel-CM: Cellular: localtime=1585038440,operator=LG U+ LGU+,loc=421E,cellid=0E38F19,mode=7
Tue Mar 24 17:27:20 2020 user.info quectel-CM: Cellular: localtime=1585038440,operator=LG U+ LGU+,loc=421E,cellid=0E38F19,mode=7
```